УДК 004.056.55:519.2

ВІДНОВЛЕННЯ S-БЛОКУ ЗА ТАБЛИЦЕЮ РОЗПОДІЛІВ ДИФЕРЕНЦІАЛІВ ТА КЛАСИ АФІННОЇ ЕКВІВАЛЕНТНОСТІ S-БЛОКІВ

С. О. Єршов[1, a]

[1] *Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського», Фізико-технічний інститут*

Анотація

Основною метою даної роботи є дослідження зв'язку між класами афінної та DDT-еквівалентності S-блоків, обчислення потужності вказаних класів еквівалентності та та експериментальна перевірка одержаних теоретичних результатів шляхом безпосередніх обчислень для S-блоків малих розмірів. Усі поставлені задачі тісно пов'язані із проблемою відновлення S-блока за його таблицею диференціальних імовірностей (DDT). Зазначена проблема добре досліджена при розгляданні диференціалів за операцією побітового додавання, але аналіз при використанні диференціалів за операцією додавання за модулем 2^n в опублікованих джерелах майже не висвітлено. У даній роботі розглядаються виключно диференціали за операцією модульного додавання.

Ключові слова: криптографія, криптоаналіз, S-блоки, DDT, відновлення S-блока, афінна еквівалентність, класи афінної еквівалентності

Вступ

На даний момент одним із найвагоміших здобутків симетричної криптології є блокові шифри, що посідають значне місце у сучасній криптології. Новітні блокові шифри розроблені на методологіях, які гарантують стійкість до відомих класичних криптоатак. У більшості випадків стійкість визначається одним з елементів блокового шифру, а саме *Substitution-блоків* (далі *S-блоки*). Зокрема, добре підібрані S-блоки можуть гарантувати стійкість шифру до лінійного та диференціального криптоаналізу, а також до ряду алгебраїчних атак.

Розроблено багато методів та інструментів для дослідження криптографічних характеристик S-блоків. Так, стійкість до диференціального криптоаналізу визначається *таблицею диференціальних імовірностей* (англ. *Difference Distribution Table*, або просто *DDT*), що містить значення імовірностей усіх диференціалів S-блоку.

На сьогоднішній день одним з розповсюджених підходів пошуку S-блоку із якісними криптографічними характеристиками полягає у випадковому генеруванні S-блоку (з урахуванням певних визначених обмежень), після чого досліджуються криптографічні параметри згенерованого перетворення, зокрема, структура DDT.

Подивимось на цей процесс з іншої сторони. Так, отримання S-блоку, що має задану DDT, є важливою практичною задачею з декількох причин.

По-перше, такий метод дає нам змогу отримувати S-блок з наперед заданими властивостями, що суттєво краще для вибору S-блоку. Таким чином, маючи алгоритм відновлення S-блока за DDT, ми можемо спочатку згенерувати DDT, що описує S-блок, який задовольняє наші потреби, після чого на основі згенерованої DDT ми можемо отримати S-блок.

По-друге, для класу криптографічних атак у моделі так званої «білої скриньки» зловмисник може отримати DDT невідомого йому S-блоку та, маючи в своєму арсеналі алгоритм для відновлення, він може отримати сам S-блок, що значно полегшує злам шифру. Відповідно, аналіз методів відновлення дозволяє оцінити стійкість криптопримітивів у моделі «білої скриньки».

Проте зауважимо, що задача відновлення S-блока за його DDT повністю не розв'язана. Основною завадою при відновленні S-блока є наявність класів афінної еквівалентності по відношенню до операції, за якої обчислюються диференціали. Афінно еквівалентні S-блоки в деяких випадках мають однакові DDT, тому не існує бієктивного відображення з множини S-блоків у множину DDT, і це значно ускладнює основну задачу.

Класичний диференціальний криптоаналіз зазвичай використовує операцію побітового додавання для обчислення різниць та диференціалів. Питанню відновлення S-блоку по DDT в цьому випадку присвячено ряд робіт, де запропоновано декілька алгоритмів різної ефективності. Виокремимо роботу [1], автори якої, Орр Дункельман та Сен'янь Хуань запропонували новий алгоритм відновлення, який грунтується на співвідношенні між DDT та таблицею лінійних апроксимацій S-блоку (Linear Approximation Table, LAT), дослідженій у [2], [3], [4]. Цей алгоритм працює краще, ніж запропонований раніше алгоритм guess-and-determine, представлений у [5].

У даній роботі ми зосередимося на диференціалах, які обчислюються відносно операції додаван-

[a] stepanersh@gmail.com

ня за модулем 2^n. Задача відновлення S-блоку за DDT при використанні операції модульного додавання в опублікованих джерелах не розглядалась, однак для окремих блокових шифрів (таких як сімейство SAFER чи алгоритм шифрування ДСТУ ГОСТ 28147:2009) саме такі диференціали розглядати більш природньо, аніж диференціали за побітовим додаванням.

Подальше викладення організоване таким чином: спочатку ми наведемо основні означення, після чого дослідимо залежність зміни DDT, побудованої на основі додавання за модулем, від афінного перетворення S-блоку. Далі буде одержано аналітичні оцінки потужностей класів афінної еквівалентності. В кінці роботи наведемо деякі практичні результати для S-блоків малої розрядності.

1. Основні означення

Наведемо основні терміни та позначення, які використовуються в даній роботі.

Через $\mathbb{F}_2^n$ позначається простір бітових векторів розмірності n, який в залежності від контексту може інтерпретуватися як кільце $\mathbb{Z}_{2^n}$; у цьому випадку двійкові вектори природним чином ототожнюються з цілими невід'ємними числами, двійковий запис яких співпадає із заданим вектором.

S-блок — це багатовимірна булева функція виду $\mathbb{F}_2^n \to \mathbb{F}_2^m$. У даній роботі розглядаються лише бієктивні S-блоки, тому, зокрема, $m = n$ (кількість вихідних змінних співпадає з кількістю вхідних). На перетворення такого типу будемо посилатись як n-бітовий S-блок.

Таблиця розподілу диференціалів (англ. the difference distribution table, DDT) S-блоку — двовимірна таблиця, кожна комірка якої містить кількість таких входів, для яких пари з різницею a переходить у пару виходів із різницею b. Для вхідної різниці $a \in \mathbb{F}_2^n$ та вихідної різниці $b \in \mathbb{F}_2^m$ комірка $\delta(a,b)$ DDT має такий вид:

$$\delta(a,b) = |\{z \in \mathbb{F}_2^n | S(z \oplus a) \oplus S(z) = b\}|,$$

де $\oplus$ — операція додавання за модулем 2 (побітового додавання). Будемо позначити DDT, побудовані таким чином, через $\mathrm{DDT}_{\oplus}$.

Зауважимо, що в деяких джерелах використовується термін «таблиця диференціальних імовірностей», оскільки DDT фактично є таблицею чисельників імовірностей усіх диференціалів S-блоку; імовірності диференціалів відповідно визначаються як $\delta(a,b) \cdot 2^{-n}$.

При використанні операції додавання за модулем 2^n таблиця розподілу диференціалів набуває іншого виду:

$$\delta(a,b) = |\{z \in \mathbb{F}_2^n | S(z+a) = b + S(z)\}|,$$

де $+$ — додавання за $\mathrm{mod} 2^n$. Такий різновид DDT будемо позначати як DDT_+.

S-блоки $S_1(x)$ та $S_2(x)$ є DDT-еквівалентними, якщо вони мають однакові DDT. У даній роботі буде розглядатись виключно DDT_+-еквівалентність.

n-бітові S-блоки $S_1(x)$ та $S_2(x)$ є афінно еквівалентними, якщо існують такі афінні бієктивні відображення A_1, A_2, що

$$S_1(x) = A_2(S_2(A_1(x))).$$

Зауважимо, що афінність розглядається по відношенню до тієї ж алгебраїчної операції, за якою обчислюються диференціали S-блоку.

2. Афінна та DDT-еквівалентність S-блоків

Як вже зазначалось, однією з основних складностей, що виникає при відновленні S-блока за його DDT_+, є той факт, що існують випадки, коли різні S-блоки мають однакову DDT_+ чи доволі схожі за тією чи іншою ознакою, що значно ускладнює поставлену задачу. Тому на практиці вводять *класи DDT-еквівалентості S-блоків.*

2.1. Зв'язок афінних перетворень та вигляду DDT

В ході аналізу предметної області даних було встановлене декілька співвідношень між DDT_+ S-блоків, що пов'язані афінними перетвореннями відносно аргументів та відносно виходів. Формалізуємо ці результати у вигляді наступних тверджень.

Твердження 1.

Нехай $S_1(x)$ та $S_2(x)$ – n-бітові S-блоки, пов'язані афінним перетворенням аргументів, тобто

$$\exists u, w \in \mathbb{Z}_{2^n} : S_1(x) = S_2(ux + w).$$

Тоді справедливе таке співвідношення між їх DDT_+:

$$\forall\ a, b \in \mathbb{F}_2^n \quad \delta_{S_1}(a,b) = \delta_{S_2}(ua, b)$$

Доведення. Маємо:

$$\delta_{S_1}(a,b) = |\{x \in \mathbb{F}_2^n \mid S_1(x+a) = S_1(x) + b\}|$$
$$= |\{x \in \mathbb{F}_2^n \mid S_2(ux + ua + w) = S_2(ux + w) + b\}|$$

Введемо заміну $y = ux + w$:

$$|\{x \in \mathbb{F}_2^n \mid S_2(y + ua) = S_2(y) + b\}| = \delta_{S_2}(ua, b),$$

що й треба було довести. □

Отже, у випадку афінного перетворення вхідних аргументів DDT_+ S-блоків однакові з точністю до перестановки рядків.

Твердження 2.

Нехай $S_1(x)$ та $S_2(x)$ – n-бітові S-блоки, пов'язані афінним перетворенням виходів, тобто

$$\exists\ u \in \mathbb{Z}_{2^n}^* \quad \exists\ w \in \mathbb{F}_2^n : S_1(x) = uS_2(x) + w.$$

Тоді справедливе таке співвідношення між їх DDT_+:

$$\forall\ a, b \in \mathbb{Z}_{2^n}^* \quad \delta_{S_1}(a,b) = \delta_{S_2}(a, u^{-1}b)$$

Доведення. Маємо:

$$\delta_{S_1}(a,b) = |\{x \in \mathbb{F}_2^n \mid S_1(x+a) = S_1(x) + b\}|$$
$$= |\{x \in \mathbb{F}_2^n \mid uS_2(x+a) + w = uS_2(x) + b + w\}|$$
$$= |\{x \in \mathbb{F}_2^n \mid uS_2(x+a) = uS_2(x) + b\}|$$

Оскільки $u \in \mathbb{Z}_{2^n}^*$, то існує u^{-1}, а тому

$$\mid S_2(x+a) = S_2(x) + u^{-1}b\}| = \delta_{S_2}(a, u^{-1}b),$$

що й треба було довести. □

Отже, у випадку афінного перетворення виходів DDT_+ S-блоків однакові з точністю до перестановки рядків.

З практичної точки зору для нас важливі такі афінні перетворення, які зберігають DDT_+. З тверджень 1 та 2 випливає, що афінні перетворення виду

$$S(x) \to S(x+a) + b,$$

де $a, b \in \mathbb{F}_2^n$, не змінюють DDT_+ S-блоку. Будемо говорити, що таке перетворення утворює *клас афінних зсувів*, а саме перетворення будемо називати *афінним зсувом*.

Однак експериментальним шляхом було встановлено, що не тільки S-блоки, що пов'язані афінними зсувами, є DDT_+-еквівалентними. Так, під час розгляду трьохбітових S-блоків було помічено, що, крім очікуваних класів DDT_+ еквівалентності потужності 64, існують класи DDT_+ еквівалентності потужності 128. Такі S-блоки пов'язані родиною афінних перетворень виду:

$$S_1(x) = 7S_2(7x + a) + b,$$

де $a, b \in \mathbb{F}_2^3$.

Таким чином, не тільки афінні зсуви зберігають DDT_+: існують афінні перетворення, в результаті яких перестановка рядків і стовпців DDT_+ утворює ту ж саму DDT_+. Пошук та повний опис таких перетворень наразі залишається відкритою задачею.

2.2. Потужність класів афінної еквівалентності

Результати, наведені у попередньому розділі, показують, що для довільного n-бітового ($n \geqslant 3$) S-блоку $S(x)$ кількість нетрівіальних афінно еквівалентних йому S-блоків, що мають таку ж саму DDT_+ з точністю до перестановки рядків та стовпців, дорівнює

$$2^{n^2}\varphi^2(2^n) = \frac{2^{n^4}}{4} = 2^{n^4-2},$$

де $\varphi(n)$ — функція Ойлера.

Для довільного n-бітового ($n \geq 3$) S-блоку $S(x)$ кількість нетрівіальних афінно-еквівалентних S-блоків, що входять до класу афінних зсувів, дорівнює 2^{n^2}.

Для наглядності, наскільки великими на практиці можуть бути класи афінної еквівалентності, наведемо числові значення потужності класів еквівалентності від розмірності S-блоку.

Результати розрахунків для классів афінної еквівалентності наведено в таблиці 1, де $|x|$ — розрядність S-блока у бітах, $\#S(x)$ — кількість S-блоків.

Табл. 1. Залежність потужності класу афінної еквівалентності від бітової розрядності S-блока

$\lvert x\rvert$	3	4	5	6
$\#S(x)$	1024	16384	262144	4194304

Табл. 2. Залежність потужності класу афінних сдвигів від бітової розрядності S-блока

$\lvert x\rvert$	3	4	5	6	7
$\#S(x)$	64	256	1024	4096	16384

Результати розрахунків потужностей класів афінних зсувів наведено у таблиці 2, що має такі самі позначення.

Висновки

У даній роботі була розглянута задача відновлення S-блоку за його таблицею розподілів диференціалів у випадку, коли диференціали обчислюються за модульним додаванням. Було показано, що певні класи афінних перетворень над $\mathbb{Z}_{2^n}$ зберігають DDT_+ — зокрема, клас афінних зсувів. Під час експериментальних обчислень класів DDT-еквівалентності трибітових S-блоків виявлено, що існують й інші типи нетривіальних афінних перетворень S-блоків, які зберігають DDT. Пошук та повний опис таких перетворень є задачею подальших досліджень.

Також необхідно зазначити, що наявність нетривіальних класів DDT-еквівалентності унеможливлює пошук окремого S-блоку за його DDT без певної додаткової інформації (наприклад, значення у деяких точках).

Перелік використаних джерел

1. Dunkelman Orr, Huang Senyang. Reconstructing an S-box from its Difference Distribution Table. — Cryptology ePrint Archive, Report 2018/811. — 2018. — `https://eprint.iacr.org/2018/811`.
2. Blondeau Céline, Leander Gregor, Nyberg Kaisa. Differential-Linear Cryptanalysis Revisited // Journal of Cryptology. — 2017. — Jul. — Vol. 30, no. 3. — P. 859–888. — Access mode: `https://doi.org/10.1007/s00145-016-9237-5`.
3. Chabaud Florent, Vaudenay Serge. Links between differential and linear cryptanalysis // Advances in Cryptology — EUROCRYPT'94 / Ed. by Alfredo De Santis. — Berlin, Heidelberg : Springer Berlin Heidelberg, 1995. — P. 356–365.
4. Blondeau Céline, Nyberg Kaisa. New Links Between Differential and Linear Cryptanalysis. — Cryptology ePrint Archive, Report 2015/183. — 2015. — `https://eprint.iacr.org/2015/183`.
5. Two notions of differential equivalence on Sboxes / Christina Boura, Anne Canteaut, Jérémy Jean, Valentin Suder // Designs, Codes and Cryptography. — 2019. — Mar. — Vol. 87, no. 2. — P. 185–202. — Access mode: `https://doi.org/10.1007/s10623-018-0496-z`.